

Opinion

A radical proposal to keep your personal data safe

Richard Stallman

The surveillance imposed on us today is worse than in the Soviet Union. We need laws to stop this data being collected in the first place

Richard Stallman is president of the Free Software Foundation

Tue 3 Apr 2018 12.05 BST



673 | 549



Journalists have been asking me whether the revulsion against the abuse of [Facebook data](#) could be a turning point for the campaign to recover privacy. That could happen, if the public makes its campaign broader and deeper.

Broader, meaning extending to all surveillance systems, not just [Facebook](#). Deeper, meaning to advance from regulating the use of data to regulating the accumulation of data. Because surveillance is so pervasive, restoring privacy is necessarily a big change, and requires powerful measures.

After the Facebook scandal it's time to base the digital economy on public ownership of data

The surveillance imposed on us today far exceeds that of the Soviet Union. For freedom and democracy's sake, we need to eliminate most of it. There are so many ways to use data to hurt people that the only safe database is the one that was never collected. Thus, instead of the EU's approach of mainly regulating how personal data may be used (in its [General Data Protection Regulation](#) or GDPR), I propose a law to stop systems from collecting personal data.

*Evgeny
Morozov*

[Read more](#)

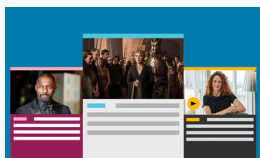
The robust way to do that, the way that can't be set aside at the whim of a government, is to require systems to be built so as not to collect data about a person. The basic principle is that a system must be designed not to collect certain data, if its basic function can be carried out without that data.

Data about who travels where is particularly sensitive, because it is an ideal basis for repressing any chosen target. We can take the London trains and buses as a case for study.

The Transport for London digital payment card system centrally records the trips any given Oyster or bank card has paid for. When a passenger feeds the card digitally, the system associates the card with the passenger's identity. This adds up to complete surveillance.

I expect the transport system can justify this practice under the GDPR's rules. My proposal, by contrast, would require the system to stop tracking who goes where. The card's basic function is to pay for transport. That can be done without centralising that data, so the transport system would have to stop doing so. When it accepts digital payments, it should do so through an anonymous payment system.

Frills on the system, such as the feature of letting a passenger review the list of past journeys, are not part of the basic function, so they can't justify incorporating any additional surveillance.



Sign up to the
Media Briefing:
news for the news-
makers

[Read more](#)

These additional services could be offered separately to users who request them. Even better, users could use their own personal systems to privately track their own journeys.

Black cabs demonstrate that a system for hiring cars with drivers does not need to identify passengers. Therefore such systems should not be *allowed* to identify passengers; they should be required to accept privacy-respecting cash from passengers without ever trying to identify them.

However, convenient digital payment systems can also protect passengers' anonymity and privacy. We have already developed one: [GNU Taler](#). It is designed to be anonymous for the payer, but payees are always identified. We designed it that way so as not to facilitate tax dodging. All digital payment systems should be required to defend anonymity using this or a similar method.

An unjust
state is more
dangerous than
terrorism, and too
much security
encourages an unjust
state

What about security? Such systems in areas where the public are admitted must be designed so they cannot track people. Video cameras should make a local recording that can be checked for the next few weeks if a crime occurs, but should not allow remote viewing without physical collection of the recording. Biometric systems should be designed so they only recognise people on a court-ordered list of suspects, to respect the privacy of the rest of us. An unjust state is more dangerous than terrorism, and too much security encourages an unjust state.

The EU's GDPR regulations are well-meaning, but do not go very far. It will not deliver much privacy, because its rules are too lax. They permit collecting any data if it is somehow useful to the system, and it is easy to come up with a way to make any particular data useful for something.

The GDPR makes much of requiring users (in some cases) to give consent for the collection of their data, but that doesn't do much good. System designers have become expert at manufacturing consent (to repurpose Noam Chomsky's phrase). Most users consent to a site's terms without reading them; a company that required users to trade their first-born child got consent from plenty of users. Then again, when a system is crucial for modern life, like buses and trains, users ignore the terms because refusal of consent is too painful to consider.

To restore privacy, we must stop surveillance before it even asks for consent.

Finally, don't forget the software in your own computer. If it is the non-free software of Apple, Google or Microsoft, it spies on you regularly. That's because it is controlled by a company that won't hesitate to spy on you. Companies tend to lose their scruples when that is profitable. By contrast, free (libre) software is controlled by its users. That user community keeps the software honest.

Richard Stallman is president of the Free Software Foundation, which launched the development of a free/libre operating system GNU

Copyright 2018 Richard Stallman. Released under Creative Commons NoDerivatives License 4.0